Hastings Law Journal

Volume 71 | Issue 2 Article 7

2-2020

The Inadequacies of the Cybersecurity Information Sharing Act of 2015 in the Age of Artificial Intelligence

Bert Lathrop

The Inadequacies of the Cybersecurity Information Sharing Act of 2015 in the Age of Artificial Intelligence

BERT LATHROP[†]

The relentless accumulation of private consumer information through online services has dramatically expanded the attack surface available to cyber-criminals and belligerent state actors looking to either enrich themselves or disrupt digital service operations. In response to this growing threat and despite sharp criticism from privacy advocates, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) with the aim of enabling private parties and the federal government to better protect themselves through improved availability of cyber threat intelligence. This intelligence is generally derived from organizations' observations of activity on their systems and networks. CISA authorizes private entities, and state, local, and tribal governments, to share cyber threat intelligence with the federal government and among themselves. In exchange, participants are granted immunity from criminal and civil liability for their acts under the statute, and the federal government publishes redacted subsets of the collected intelligence.

Coincidentally, artificial intelligence (AI) has recently emerged as a technology showing great promise in automating many tasks currently performed by humans, and cybersecurity analysis is no exception. CISA, drafted concurrently with this emergence, lacks the data-sharing authorizations necessary to leverage AI's full utility. Deep learning, the AI technology showing the most promise, requires vast amounts of data providing evidence of normal system and network activity from which anomalous events associated with cyber-attacks can be differentiated. While CISA authorizes the sharing of the requisite data for such analyses in limited circumstances, this Note explores the opportunities AI affords cybersecurity practitioners, explains the shortcomings of CISA with respect to enabling AI to approach its full potential in cybersecurity applications, and offers a remedial proposal to those shortcomings.

[†] Bert Lathrop is a 3L at the University of California, Hastings College of the Law. Prior to enrolling at U.C. Hastings, Bert was co-founder and Chief Operating Officer of Farsight Security, Inc., a cybersecurity firm that provides its subscription clients with cyber threat intelligence derived from global DNS transaction observations. Bert earned his M.B.A. degree from the N.Y.U. Stern School of Business, the London School of Economics and Political Science, and the HEC Paris School of Management, and his Bachelor of Science degree in Computer Information Systems, *summa cum laude*, from Excelsior College.

TABLE OF CONTENTS

INTRODUCTION

As the new millennium dawned, "about half of all adults were already online. Today, roughly nine-in-ten American adults use the [I]nternet."[1] Since 2000, the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), "received more than 4 million victim complaints . . . . [In 2017 alone, the IC3] received more than 300,000 complaints . . . with reported losses of more than $1.4 billion."[2] In response to the escalating rate of Internet crime, circa 2011, Congress began reviewing a number of proposals aimed at improving the availability of cyber threat intelligence to the private and public sectors.[3]

> While considerable debate exist[ed] with regard to the best strategies and methods for protecting America's various cybersystems, one point of "general agreement" among cyber-analysts [was] the perceived need for enhanced and timely exchange of cyber threat intelligence both within the private sector and between the private sector and the government.[4]

In December 2015, after much contentious debate at a policy level between security and privacy advocates,[5] and at the solution level between proponents of various alternative bills,[6] President Obama signed the Cybersecurity Information Sharing Act of 2015 (CISA) into law.[7]

To understand how CISA can affect cybersecurity effectiveness, it helps to have a basic understanding of how the Internet is organized. The Internet is generally composed of a multitude of private networks interconnected through the services of Internet service providers, or ISPs, and other backbone network providers. These many private networks are protected by cybersecurity practitioners through the use of a cybersecurity infrastructure, which requires detailed threat intelligence to allow bona fide users access to services while barring likely nefarious actors from harming the organization's systems. Analogizing to castle defenses, CISA authorizes individual private castle owners to share cyber threat intelligence with other castle owners and with the federal government information regarding the identity of such nefarious actors, their modus operandi, and how to defend against their attacks. It also authorizes castle

---

1. *Internet/Broadband Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), http://www.pewinternet.org/fact-sheet/internet-broadband/.

2. *Latest Internet Crime Report Released: IC3 Says Victim Losses Exceeded $1.4 Billion in 2017*, FBI NEWS (May 7, 2018), https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718).

3. ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS 43–58 (2015).

4. *Id.* at 3–4 (citing BIPARTISAN POLICY CTR., CYBER SECURITY TASK FORCE: PUBLIC-PRIVATE INFORMATION SHARING 5 (July 2012), https://bipartisanpolicy.org/wp-content/uploads/2019/03/Public-Private-Information-Sharing.pdf).

5. *See infra* Subpart I.B.3.

6. *See* NOLAN, *supra* note 3, at 43–58.

7. 6 U.S.C. §§ 1501–10 (2018). *See* Andy Greenberg, *Congress Slips CISA into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015, 12:24 PM), https://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Everett Rosenfeld, *The Controversial "Surveillance" Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), https://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

owners to monitor their respective castle walls, wall perimeters, and the space within their individual castles for discreet evidence of activity, equivalent to footprints in the snow that may provide clues about users' activity, whether well-intended or not. CISA does not authorize any castle owner to send any such evidence to other castle owners, but castle owners may authorize third parties—presumably cybersecurity firms—to monitor those specific castles on behalf of their owners. This last authorization positions such third parties to accumulate and analyze evidence collected across all the castle defenses for which they are responsible, thus providing them with a unique bird's-eye view of footsteps left in the snow not afforded to any individual castle owner unless they subscribe to such a cybersecurity firm's services.[8]

Although debates were very active between CISA proponents and privacy advocacy organizations prior to the passage of CISA,[9] comparatively little has been written about it since.[10] CISA was designed to address the government's and the private sector's needs for sharing information related to perceived cyber threats and related defensive measures, but it was not drafted with modern data science in mind, particularly artificial intelligence (AI). This Note takes a critical view of the authorizations and legal immunities afforded by CISA in light of the unforeseen risks and opportunities introduced by the advent of AI and its applications to the domain of cybersecurity.

Part I provides a primer on the cybersecurity vocabulary necessary to appreciate the finer points of the argument of this Note, relevant provisions of CISA, and the context in which that statute was enacted, including the cyber threats our nation faced during the years leading up to its passage. Part II provides a perspective on the post-CISA cybersecurity context, including the ever-evolving cyber threat landscape, liability concerns that continue to chill participation in cyber threat intelligence sharing despite the legal immunities afforded by CISA, the advent of AI including its introduction into the cyber threat mix, and staffing issues facing organizations attempting to defend themselves in the context of an escalating cyber threat landscape. Part III outlines a proposal calling for new legislation that would amend CISA by expanding its data sharing authorization to include raw observational evidence of system and network activity between non-federal entities, and by refining the definition of personally identifiable information and limiting the sharing authorization for such information. Using a review and analysis of a similar data

8. While such a limitation may seem unfortunate, a statutory interpretation of CISA helps understand the tension between security and privacy interests that likely led to this limitation. *See infra* Subpart I.C.4.

9. The American Civil Liberties Union and the Electronic Frontier Foundation actively argued against the passage of this legislation. *See infra* Subpart I.B.3.

10. Westlaw indicates no activity before the courts in relation to CISA, and only two law journal articles or notes appear to have been written about it. John Heidenreich, Note, *The Privacy Issues Presented by the Cybersecurity Information Sharing Act*, 91 N.D. L. REV. 395 (2015) (discussing privacy concerns with CISA's data sharing authorizations); Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C. L. REV. 585 (2016) (discussing shortcomings related to the mechanics of execution of the functions authorized under CISA).

sharing proposal in the context of the European General Data Protection Regulation (GDPR) legislation, this Part further demonstrates that the proposed data sharing enhancements are in the public interest, thus providing a counterargument to the concerns that privacy advocates would likely raise.

Areas of additional possible research that are not within the scope of this Note include, but are not limited to, privacy-preserving data mining techniques in cybersecurity,[11] policies such as retention periods and security requirements to be applied to shared cyber threat intelligence data, and the logistics that should enable non-federal entities in sharing data.

I. THE LANGUAGE AND CONTEXT OF CISA

This section provides a primer on the cybersecurity vocabulary necessary to appreciate the finer points of this Note's argument, as well as an overview of the context of the enactment of CISA and some of its relevant provisions.

A. CYBERSECURITY—SELECT DEFINITIONS

One challenging aspect of understanding cyber law is the degree of complexity of the technology and its unfamiliar jargon. Cybersecurity comes with a dense vocabulary of its own, evidenced by the more than two-hundred-page information security glossary documented by the Information Technology Laboratory of the National Institute of Standards & Technology.[12] The following are some definitions of terms useful for understanding CISA and its impact on cybersecurity.

1. Cybersecurity Infrastructure

Conceptually very broad, cybersecurity infrastructure "[i]ncludes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements."[13] The physical elements of a well-appointed cybersecurity infrastructure include common servers and network routing and switching components, but may also include special-purpose cybersecurity

11. *See, e.g.*, SUMEET DUA & XIAN DU, DATA MINING AND MACHINE LEARNING IN CYBERSECURITY 177–203 (2011).

12. *See generally* RICHARD KISSEL, NAT'L INST. OF STANDARDS AND TECH., NISTIR 7298, GLOSSARY OF KEY INFORMATION SECURITY TERMS (2013) (archived publication). The National Institute of Standards and Technology is an organization whose mission is "to promote U.S. innovation and industrial competitiveness by advancing . . . standards" in information technology. *NIST General Information*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/director/pao/nist-general-information (last visited Jan. 24, 2020).

13. KISSEL, *supra* note 12, at 58.

appliances, such as firewalls,[14] intrusion detection systems,[15] or cloud-based cybersecurity services, like file reputation services.[16]

2. Cyber Threat Intelligence

In his research at the SANS Institute, Greg Farnham defined cyber threat intelligence as "threat intelligence related to computers, networks and information technology."[17] It is "the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding, [and] is the product that provides battlespace awareness."[18]

Cyber threat intelligence is produced through the analysis of large quantities of raw data and information, producing relevant, actionable intelligence, but raw data and information alone do not constitute cyber threat intelligence.[19] Depending on the form of analysis used to produce it, cyber threat intelligence falls into three broad categories: strategic, tactical, and operational.[20]

"Strategic threat intelligence is a bird's-eye view of an organization's threat landscape. Not concerned with specific actors, indicators, or attacks, it instead aims to help high-level strategists understand the broader impact of business decisions [on the cybersecurity posture of an organization]."[21]

> Tactical threat intelligence provides information about the tactics, techniques, and procedures . . . used by threat actors to achieve their goals (e.g., to compromise networks, exfiltrate data, and so on). It's intended to help defenders understand how their organization is likely to be attacked, so they can determine whether appropriate detection and mitigation mechanisms exist or whether they need to be implemented.[22]

"Operational threat intelligence relates to specific attacks or campaigns. It helps defenders understand the nature, intent, and timing of a specific attack . . . provides insight into the nature and sophistication of the group(s) responsible,"[23] and focuses on the discrete data elements that identify threats to an organization's information processing infrastructure, applications, and data.

---

14. *Id.* at 79.

15. *Id.* at 104.

16. *See, e.g.*, *TITANIUMCLOUD: File Reputation*, REVERSINGLABS, https://www.reversinglabs.com/products/file-reputation-service (last visited Jan. 24, 2020).

17. GREG FARNHAM, TOOLS AND STANDARDS FOR CYBER THREAT INTELLIGENCE PROJECTS 8 (2013), https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375.

18. *Id.* (citing EDWARD WALTZ, INFORMATION WARFARE PRINCIPLES AND OPERATIONS (1998)).

19. Zane Pokorny, *What Is Threat Intelligence? Definition and Examples*, RECORDED FUTURE (Apr. 30, 2019), https://www.recordedfuture.com/threat-intelligence-definition/.

20. *Id.*

21. *How Strategic Threat Intelligence Informs Better Security Decisions*, RECORDED FUTURE (Sept. 13, 2018), https://www.recordedfuture.com/strategic-threat-intelligence/.

22. *Id.*

23. *How Operational Threat Intelligence Blocks Attacks Before They Happen*, RECORDED FUTURE (Sept. 25, 2018), https://www.recordedfuture.com/operational-threat-intelligence/.

A key distinction between operational and strategic cyber threat intelligence is that the former endeavors to discover and catalog nefarious actors' technical specifics including IP addresses, email addresses, or modus operandi to later inhibit any cyber-attacks those actors may attempt to perpetrate, whereas the latter is a narrative of the aspects of an organization that would likely cause, or at least promote, the existence of a threat without knowing of any specific threat attributes.

If the computer systems and special purpose appliances that make up an organization's physical cybersecurity infrastructure and the cybersecurity-specific applications hosted by those systems altogether are the engines that power cyber-defense capability, then it is easy to think of operational threat intelligence as the data necessary to direct or target the efforts of those engines.

a. Cyber Threat Indicators (CTIs)

A type of operational cyber threat intelligence, CTIs are the sets of data elements necessary to describe or identify a threat or risk to computer systems or networks. They may include any combination of an identifiable pattern of[24]:

- malicious network reconnaissance activity,[25]
- a malicious cyber command and control,[26]
- a method for defeating security controls,[27]
- a security vulnerability,

24. DEP'T. OF HOMELAND SEC. & DEP'T. OF JUSTICE, FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT 13 (2016) [hereinafter DHS & DOJ].

25. *See generally* H. P. Sanghvi & M. S. Dahiya, *Cyber Reconnaissance: An Alarm Before Cyber Attack*, 63 INT'L J. COMPUTER APPLICATIONS 36 (2013).

26. Botnets are autonomous, drone-like programs that, once infiltrated and installed in a target environment, act under the direction of a malicious cyber command and control (C&C) that instructs them through communication pathways that range from the very simple to the arbitrarily complex. *E.g.*, *GameOver Zeus Botnet Disrupted: Collaborative Effort Among International Partners*, FBI NEWS (last updated July 11, 2014), https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted; *see* DUA & DU, *supra* note 11, at 209–11 (2011) (detailing, in section 9.1.2, general characteristics of botnet detection and eradication methods); DHS & DOJ, *supra* note 24, at 14. An initial bot is generally introduced into the target organization through some form of malicious code attack, for example, a phishing campaign that infects one or more computers in the target network. Once introduced, the bot spreads through the target computer network like a virus, replicating itself across computer systems by leveraging one or more known system vulnerabilities. The bots then persist on the infected systems, awaiting the receipt of instructions from the malicious C&C, whether by reaching back out periodically to a pre-configured URL or IP address, see KISSEL, *supra* note 12, at 104, or indirectly through another infected system as with the GameOver Zeus botnet. A CTI documenting the details of a botnet would, of course, include such details as the malicious code CTI that introduces the botnet, the URL(s) and/or IP addresses to which the bots connect or the algorithm by which they calculate these at any given moment, and a narrative describing the behavior and nefarious effects of the botnet. This definition is not intended to provide a complete typology of possible botnet configurations, but rather to demonstrate that URLs and IP addresses are fundamental to the description of a botnet CTI.

27. S*ee* KISSEL, *supra* note 12, at 175–76.

- a method for causing a legitimate user to unwittingly defeat a security control,[28]
- the actual or potential harm caused by a cybersecurity incident including any data exfiltrated as a result,[29] or
- "any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law."[30]

The discrete data elements used to document a CTI may include indicators of compromise (IOCs)[31] or any other raw data necessary to adequately complete the characterization of the threat or risk.

CTIs may describe any matter of cyber-risk, including malicious code or malware,[32] a phishing attack, or a botnet. A CTI is a complex data structure that

---

28. A user may unwittingly defeat an organization's security controls by falling victim to a phishing attack. *See* KISSEL, *supra* note 12, at 142; *see also* DUA & DU, *supra* note 11, at 208 (describing, at section 9.1.1, a phishing attack resulting in the introduction of malware onto a user's system). Such attacks may be broad, that is, sent to a large email list purchased on the black market, or narrowly targeted at select individuals within an organization after extensive research into their personal details, which is considered a more insidious activity known as spear phishing. *E.g.*, Sean Michael Kerner, *Sony Hackers Used Apple ID Phishing Scheme, Researchers Claim at RSA*, EWEEK (Apr. 21, 2015), http://www.eweek.com/security/sony-hackers-used-apple-id-phishing-scheme-researchers-claim-at-rsa. Invariably, the email will contain a URL, *see* Memorandum from Tim Berners-Lee, et al., on Uniform Resource Locators (URL) to Networking Working Group (Dec. 1994), https://www.ietf.org/rfc/rfc1738.txt, or a website link the receiver is invited to click, which then takes her to a malicious website soliciting her personal details. *E.g.*, *The Phishing Email That Hacked the Account of John Podesta*, CBS NEWS (Oct. 28, 2016, 11:43 AM), https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/. A phishing attack CTI would include the email envelope or header including the sender's email address, the email body including the malicious URL, and a narrative of the behavior of the malicious website or resource linked to the malicious URL. Methods for gathering the data necessary to populate a phishing CTI include human intelligence, for example, the email recipient comparing the URL to what he knows to be valid in context and reporting a suspicious email to his cybersecurity team; policy-based screening automation, that is, the email recipient clicks the URL link and is protected by infrastructure designed to block and report against entire classes of high-risk Internet domain names, *see, e.g.*, *Newly Observed Domains: Threat Protection from New Domains*, FARSIGHT SECURITY, https://www.farsightsecurity.com/solutions/threat-intelligence-team/newly-observed-domains/ (last visited Jan. 24, 2020), or detailed forensic analysis of a particular phishing attack a specific user has experienced.

29. *See Exfiltration: The Adversary Is Trying to Steal Data*, MITRE, https://attack.mitre.org/tactics/TA0010/ (last visited Jan. 24, 2020) (providing a definition for exfiltration and examples of techniques).

30. *See* DHS & DOJ, *supra* note 24, at 13.

31. *See infra* Subpart I.A.1.c.

32. A CTI describing malicious code or malware would likely include such IOCs as the name of the file containing the malicious code, the file size, and a uniquely identifying signature of the file. *See* DUA & DU, *supra* note 11, at 208 (describing, in section 9.1.1, a phishing attack resulting in the introduction of malware onto a user's system); *see also* KISSEL, *supra* note 12, at 84, 118. In such a CTI, IOCs would likely be accompanied by a narrative detailing the nefarious behavior of the malware. *E.g.*, *Reports*, VIRUSTOTAL, https://support.virustotal.com/hc/en-us/articles/115002719069-Reports (last visited Jan. 24, 2020) (detailing the elements of a sample malicious code attack signature). A malware CTI generally results from a static analysis of the file content and/or dynamic observation of the malicious code's behavior in an isolated execution environment or sandbox. *E.g.*, *Active File Decomposition*, REVERSINGLABS, http://reversinglabs.com/technology/active-file-decomposition.html (last visited Jan. 24, 2020) (detailing technology capable of decomposing a file down to discrete instructions in order to detect malicious fragments within); *Symantec Content & Malware Analysis*, SYMANTEC, https://www.symantec.com/products/atp-content-malware-analysis (last visited Jan. 24, 2020); *see also* KISSEL, *supra* note 12, at 168 (detailing file behavior analysis in a quarantined computing environment).

often requires significant analysis before a cybersecurity analyst can complete its documentation. CTIs are composed of IOCs, which may contain personally identifiable information (PII),[33] and are accompanied by a narrative putting those IOCs in the context of the threat described.

Once compiled, CTIs are shared with peers either directly or through community sharing schemes, including the federal government as authorized under CISA.[34] CTI recipients, now informed of the characteristics of a given cyber threat, can use this information to develop defensive measures and configure them into their systems and cybersecurity infrastructure to defeat the threat detailed in the CTI.[35]

b. Defensive Measures (DMs)

Like CTIs, DMs are also a form of operational cyber threat intelligence. Once a CTI is documented, a related DM might also be documented, detailing inhibiting or defensive tactics to protect against the threat defined in the CTI, if those details are known. For example, a DM for a phishing threat would likely include instructions to simply inhibit any outbound connection requests to the malicious URL detailed in the CTI for that phishing attempt. Similarly, the DM for a particular element of malicious code might include clues for detecting the file, such as the unique signature identifying the file, and instructions for placing the malicious elements of that code in quarantine on infected systems. Sharing DMs among cyber threat analysts allows the research performed by one to be leveraged by many, thus improving the efficiency of devising and deploying proven cyber defenses.

---

33. For example, email or IP addresses. Personally identifiable information (PII) definitions vary by jurisdiction. Notable definitions include those of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA). The GDPR defines "personal data" as:

> [A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 33. The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," and supplements that definition with a non-exhaustive list of examples of the types of information that constitute personal information. CAL. CIV. CODE § 1798.140(o)(1) (West 2019). The inclusion of PII in CTIs fuels the debate between privacy advocates who would prefer that no such data be shared for the sake of privacy, and security minded practitioners who suggest that the effectiveness of cybersecurity defenses is enhanced by the availability of data that provide situational awareness. *See infra* Subpart I.B.3.

34. *See infra* Subpart I.C.

35. *See infra* Subpart I.A.1.b.

c. Indicators of Compromise (IOCs)

Greg Farnham defines IOCs as "one of the most easily actionable types of [cyber threat intelligence] . . . . Some of the most commonly used IOCs are IP addresses, domain names, uniform resource locators (URLs) and file [signatures]."[36] They are the results of detailed analyses sufficient to draw a judgment of potential threat or risk. As IOCs are attack-specific, they are not particularly useful or actionable absent the context of the attack where they were observed. For example, an email address in and of itself is not actionable, but that same address can be added to an email blocking list as a DM if that email address has been identified as the source of a phishing attack. Further examples of the operational use of IOCs include using a list of file signatures associated with files known to contain malicious code to inform an anti-virus application or using a blacklist of threatening URLs to inhibit user connections to the Internet resources associated with those URLs. IOCs are critical to cyber defense, as they are the necessary data cyber-analysts use to configure the cybersecurity infrastructure guarding an organization's systems and networks.

3. Raw Observational Data (ROD)

It is common practice in network and data center operations to log detailed user system and network activity (raw observational data or ROD). While ROD is not a concept exclusive to cybersecurity or to its vocabulary, for the purposes of this Note, ROD is defined as the data collected as trace evidence of activity on an organization's systems and networks. Systems operations support staff and cybersecurity analysts routinely analyze ROD in support of their respective functions, including real-time surveillance activities, forensic investigations, and the documentation of CTIs and cyber-crime reports for law enforcement.[37]

One may liken ROD, which may include email addresses, domain names, URLs, or IP addresses, to footprints left in the snow by those interacting with an organization's systems and networks. As these footprints may be evidence of the identity of the actor communicating with the organization in that moment, they can be very useful to a cybersecurity analyst to track down a nefarious actor who has infiltrated an organization's network and system resources, or otherwise attribute a cyber-crime to its perpetrator. Unlike a CTI, ROD does not associate any judgment of risk or attribution with the data elements within it; its presence in a log file or data stream is a mere fact of recorded system and network activity history.

A specific example of ROD with direct applicability to cybersecurity is "passive DNS" data,[38] evidence of a query-response exchange between an

36. FARNHAM, *supra* note 17, at 8.

37. *Id.* at 9.

38. *See* Cricket Liu, *Strengthen Your Network Security with Passive DNS*, INFOWORLD (Oct. 20, 2015), https://www.infoworld.com/article/2994016/network-security/strengthen-your-network-security-with-passive-dns.html; *see also* FLORIAN WEIMER, PASSIVE DNS REPLICATION (2005), https://www.first.org/conference/2005/papers/florian-weimer-paper-1.pdf.

organization's network infrastructure and the global Domain Name System (DNS).[39] Such exchanges happen routinely as an organization's users attempt to access Internet resources previously unknown to the organization's network.[40] Being able to look retrospectively at the evidence of such exchanges is invaluable to investigating a cyber-attack,[41] such as in the case of a phishing attack where a new nefarious domain name was presented to an unsuspecting user, inviting the user to access the domain to initiate the phishing attack.[42]

While CISA specifically authorizes the sharing of CTIs and DMs among various stakeholders, it does not authorize the sharing of ROD except in the very narrow circumstance of an authorized third-party network monitoring activity.[43] The specific reasons for the exclusion of such valuable data from the sharing authorization provisions are not known with precision, but the compromise between security- and privacy-minded arguments likely explain it.[44]

Under CISA, unless necessary to properly document a CTI or DM, PII must be redacted before either type of report is shared.[45] On the other hand, as ROD most often documents evidence of a specific user's system and network activity, it must contain a modicum of PII lest it be rendered valueless. As a result, organizations collecting ROD and their system users harbor much greater privacy concerns regarding ROD as its content is often more sensitive than that of CTIs or DMs from which all unnecessary PII must be redacted under CISA.[46]

B. CYBERSECURITY RISKS PRIOR TO 2015 AND THE CONGRESSIONAL RESPONSE

1. Cyber-Crimes Moved to the Headlines

During the years leading up to the fall of 2015, a number of high-profile cyber-attacks were perpetrated against prominent U.S. corporations and government agencies.[47] The most prominent of these attacks, the Anthem data

39. Memorandum from Paul Mockapetris on Domain Names—Implementation and Specification to Network Working Group (Nov. 1987), https://www.ietf.org/rfc/rfc1035.txt.

40. *Id.*

41. Commercial cybersecurity companies harvest Passive DNS data across many organizations' networks to create a database providing a time-series, composite view of the content of the global Domain Name System in support of complex, cross-network forensic investigations. *See e.g.*, *Plug into the World's Largest DNS Intelligence Solution: DNSDB*, FARSIGHT SECURITY, https://www.farsightsecurity.com/solutions/dnsdb/ (last visited Jan. 24, 2020). Such databases do not provide any form of risk scoring associated with an IOC, but may answer questions regarding a suspect domain name, including IP addresses that have historically hosted the domain, or the set of other domains that are or have been hosted on a same IP network address range, that is, known associates in law enforcement parlance. *Id.*

42. *See supra* note 28 (explaining the risks associated with phishing attacks).

43. *See infra* Subpart I.C (providing an overview of the relevant provisions of CISA).

44. *See infra* Subpart I.B.3 (outlining the controversies surrounding the passage of CISA and the resulting compromise provisions of the bill).

45. *See infra* Subpart I.C.

46. *See infra* Subpart I.C.

47. *E.g.*, Jim Finkle, *Hackers Raid eBay in Historic Breach, Access 145 Million Records*, REUTERS (May 21, 2014, 8:01 PM), https://uk.reuters.com/article/uk-ebay-password/hackers-raid-ebay-in-historic-breach-

breach perpetrated by two Chinese nationals, was documented in a federal grand jury indictment unsealed in 2019.[48] Tens of millions of credit card numbers were stolen in a single attack on the Target store chain,[49] and several such attacks were successful against a variety of large store chains and retail banks.[50] Agents acting on behalf of the North Korean government allegedly attacked the Bank of Bangladesh, making away with $81 million.[51] And "[i]n perhaps the most infamous cyberattack of 2014 . . . Sony Pictures Entertainment suffered a 'significant system disruption' as a result of a 'brazen cyber-attack' [also attributed to the North Korean government] that resulted in the leaking of personal details of thousands of Sony employees."[52]

The public felt the impact of these cyber-attacks directly as they jeopardized health records, financial data, or other private information of hundreds of millions of U.S. residents. As a result, the reality of cyber-risk moved front and center in the public debate. Although cybersecurity practitioners continued to cite current and former employees most frequently as the culprits for cybersecurity incidents,[53] this time period saw a marked acceleration in attacks attributable to organized crime and nation-state actors.[54]

2. Early Attempts to Implement Legislative Solutions Fail

Between 2011 and 2014, a number of bills aimed at providing a statutory framework for the exchange of cyber threat intelligence between the private sector and the federal government were introduced in both houses of Congress.[55]

---

access-145-million-records-idUKKBN0E10ZL20140522; Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2015), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?utm_term=.2ac; Ellen Nakashima, *Hackers Breach Some White House Computers*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fdd580f1c5d44e_story.html; Gregory Wallace, *Target Credit Card Hack: What You Need to Know*, CNN MONEY (Dec. 23, 2013, 11:43 AM), https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html; Michael Winter, *Home Depot Hackers Used Vendor Log-On to Steal Data, E-mails*, USA TODAY, https://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/ (last updated Nov. 7, 2014, 8:57 AM).

48. Nicole Perlroth, *Two From China Are Charged in 2014 Anthem Data Breach*, N.Y. TIMES (May 9, 2019), https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html?searchResultPosition=1.

49. *See* Wallace, *supra* note 47.

50. *See supra* note 47.

51. Criminal Complaint at 3, United States v. Park Jin Hyok, No. MJ18-1479 (C.D. Cal. June 8, 2018).

52. NOLAN, *supra* note 3, at 1 (quoting Press Release, Sony Pictures Entertainment, Message for Current and Former Sony Pictures Employees and Dependents, and for Production Employees (Dec. 15, 2014), http://www.sonypictures.net/SPE_Cyber_Notification.pdf?) (citing Amelia Smith, *Sony Cyber Attack One of Worst in Corporate History*, NEWSWEEK (Dec. 4, 2014, 1:14 PM), http://www.newsweek.com/sony-cyber-attack-worst-corporate-history-thousands-files-are-leaked-289230).

53. PWC, MANAGING CYBER RISKS IN AN INTERCONNECTED WORLD: KEY FINDINGS FROM THE GLOBAL STATE OF INFORMATION SECURITY SURVEY 2015 13 (2014).

54. *See id.* at 15.

55. *See* NOLAN, *supra* note 3, at 43 n.345.

For example, in late 2011, the Cyber Intelligence Sharing and Protection Act (CISPA) was introduced to the U.S. House of Representatives.[56] Despite a strong consensus and bipartisan approval in the U.S. House of Representatives,[57] the U.S. Senate defeated CISPA through a filibuster, citing its lack of specific protection for critical infrastructure.[58]

The Snowden disclosures of 2013 appeared to dramatically change the political climate surrounding cybersecurity legislation.[59] The public had learned of the federal government's widespread data collection and surveillance strategies, which cast a notable chill on any bills advocating the sharing of cyber threat intelligence with the federal government.[60] Further, those disclosures incentivized privacy advocates to redouble their lobbying efforts.[61] As a result, until 2015, bills aiming to authorize the sharing of cyber threat intelligence with the federal government were defeated on the grounds of privacy concerns, which were acknowledged by both sides of the aisle and by President Obama.[62]

3. CISA Enacted in 2015 Despite Significant Privacy Concerns

Despite its many failed attempts to pass legislation to improve the nation's cyber threat intelligence capabilities, Congress continued its efforts to find a solution. As indicated in the Senate report on the activities of the Select Committee on Intelligence covering the period of January 6, 2015 to January 2, 2017, "[b]uilding on the [Intelligence] Committee-reported Cyber Information Sharing Act (CISA) during the 113th Congress, the Committee reported an updated Cybersecurity Information Sharing Act of 2015 (S. 754) on March 17, 2015. The bill included authorizations, procedures, and protections to encourage public/private collaboration on cybersecurity threats."[63]

The shaping and ultimate passage of CISA proved particularly controversial.[64] The U.S. Chamber of Commerce came out in favor of the bill,

---

56. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011).

57. Robert Pear, *House Votes to Approve Disputed Hacking Bill*, N.Y. TIMES (Apr. 26, 2012), https://www.nytimes.com/2012/04/27/us/politics/house-defies-veto-threat-on-hacking-bill.html.

58. Michael S. Schmidt, *Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster*, N.Y. TIMES (Aug. 2, 2012), https://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.

59. *See* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded: What the Revelations Mean For You*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

60. Robert X. Cringely, *NSA, PRISM, and CISPA: The Conspiracy Behind the Conspiracy*, INFOWORLD (June 14, 2013), https://www.infoworld.com/article/2611569/nsa--prism--and-cispa--the-conspiracy-behind-the-conspiracy.html.

61. *See, e.g.*, CISPA Is Back, ELEC. FRONTIER FOUND., https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=9048 (last visited Jan. 24, 2020).

62. *See* Kate Knibbs, *The New CISPA Bill Is Literally Exactly the Same as the Last One*, GIZMODO (Jan. 14, 2015, 2:25 PM), https://gizmodo.com/the-new-cispa-bill-is-literally-exactly-the-same-as-the-1679496808; Michelle Richardson, *Opposition to CISPA Is Growing!*, AM. CIVIL LIBERTIES UNION (Apr. 24, 2012, 1:01 PM), https://www.aclu.org/blog/national-security/opposition-cispa-growing.

63. S. REP. NO. 115-13, at 2 (2017).

64. *See* Andy Greenberg, *CISA Security Bill: An F for Security But an A+ for Spying*, WIRED (Mar. 20, 2015, 7:00 AM), https://www.wired.com/2015/03/cisa-security-bill-gets-f-security-spying/; Andy Greenberg,

suggesting that it was the progress the United States required to improve the security of its businesses and government.[65] Privacy advocacy groups such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) each expressed strong opposition to the bill, citing grave privacy concerns with CISA's new data sharing authorizations.[66] A group of cybersecurity professionals and other technologists joined the chorus of dissenters, suggesting that the privacy risks introduced by CISA were not worth the limited value of CTIs and DMs to their cybersecurity analysis needs.[67] Likewise, a diverse group of large Silicon Valley tech companies, which safeguard a great deal of private consumer data, were eager to demonstrate their support for individual privacy rights by lobbying against the bill.[68]

On April 15, 2015, the Senate Select Committee on Intelligence recommended the passage of CISA.[69] The divergent opinions of security-conscious and privacy-conscious stakeholders were clearly reflected in the committee report. On the one hand, Senators Heinrich and Hirono felt compelled to note that, while they supported the "broad aims" of the bill, it

> [P]rovides more restraints, guidance, and oversight than did the earlier draft version of the legislation, including a narrowing of the definition and authorized use of defensive measures, fewer exceptions for liability protections for information shared outside of the DHS portal, and more limits on how cyber threat information is used.[70]

On the other hand, Senator Wyden voiced his dissent in opposition to the bill, suggesting he believed the bill's "insufficient privacy protections will lead to large amounts of personal information being shared with the government even when that information is not needed for cybersecurity. This could include email

---

Congress Slips CISA into a Budget Bill That's Sure to Pass, WIRED (Dec. 16, 2015, 12:24 PM) [hereinafter Greenberg, *Congress Slips CISA*], https://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Peter Hess, *Controversial New Cybersecurity Law May Compromise Privacy*, SCIENCELINE (Jan. 24, 2016), https://scienceline.org/2016/01/controversial-new-cybersecurity-law-may-compromise-privacy/.

65. Press Release, U.S. Chamber of Commerce, U.S. Chamber's Donohue: 'CISA is a Positive Step Forward on Cybersecurity' (Oct. 27, 2015, 5:15 PM), https://www.uschamber.com/press-release/us-chamber-s-donohue-cisa-positive-step-forward-cybersecurity.

66. Letter from Karin Johansen, Dir., Wash. Legislative Office, & Gabriel Rottman, Legislative Counsel/Policy Advisor, to U.S. Senators, Vote NO on the Motion for Cloture for S. 754, the Cybersecurity Information Sharing Act of 2015 (Oct. 22, 2015) https://www.aclu.org/letter/aclu-vote-recommendation-urging-senate-vote-no-cloture-motion-s-754-cybersecurity-information; Mark Jaycox, *EFF Opposes Cybersecurity Bill Added to Congressional End of Year Budget Package*, ELEC. FRONTIER FOUND., (Dec. 18, 2015), https://www.eff.org/deeplinks/2015/12/statement-finalized-congressional-cybersecurity-bill.

67. Letter from Ben Adida et al., to Senators Feinstein & Burr, and Representatives Schiff, Nunez, & McCaul (Apr. 16, 2015) http://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf.

68. *See, e.g.*, Sam Thielman, *Apple, Google and Twitter Among 22 Tech Companies Opposing CISA Bill*, GUARDIAN (Oct. 21, 2015), https://www.theguardian.com/technology/2015/oct/21/apple-google-and-twitter-among-22-tech-companies-opposing-cisa-bill ("The trust of our customers means everything to us and we don't believe security should come at the expense of their privacy.").

69. S. REP. NO. 114-32, at 1 (2015).

70. *Id.* at 17.

content, financial records, and a wide variety of other personal information."[71] These senators felt compelled to register their respective points, which live at opposite ends of the spectrum in the security-privacy balance, suggesting that the content of the bill was a compromise of opposing views.

Nevertheless, on October 27, 2015, the Senate passed CISA by a vote of seventy-four to twenty-one and, in an effort to end debate and overcome a threatened presidential veto, "it was incorporated into and became law as part of H.R. 2029 [the $1.1 trillion 2016 omnibus funding bill] on December 18, 2015."[72] Despite the chilled climate brought on by the Snowden disclosures, the escalating headlines describing one more devastating cyber-crime after the next likely incentivized Congress to act, passing a particularly controversial piece of legislation.

C. RELEVANT CISA PROVISIONS

CISA establishes a cyber threat intelligence sharing scheme between the federal government, and private entities, state, local, and tribal governments (all together "non-federal entities" or "NFEs"),[73] and among NFEs. Program participants are provided with broad liability protection for their actions under the statute.

1. Role of the Department of Homeland Security

CISA designates the Department of Homeland Security (DHS) as the agency with operational responsibility for a cybersecurity information sharing service.[74] Through this service, the DHS is required to process the receipt of [CTIs] and [DMs] from NFEs "through an automated real-time exchange, electronic mail or media, or a website interface."[75] Further, the DHS is required to publish, in real-time if possible, various subsets of the cyber threat intelligence it receives under CISA to NFEs and appropriate federal agencies,[76] depending on their respective levels of security clearance.[77]

2. Authorization to Share CTIs and DMs and to Monitor Systems

Under CISA, NFEs are authorized to share CTIs and DMs with the federal government and/or with other NFEs for cybersecurity purposes only.[78] They are

71. *Id.* at 21.

72. S. REP. NO. 115-13, at 3 (2017); *see also* 6 U.S.C. §§ 1501–10 (2018); Greenberg, *Congress Slips CISA*, *supra* note 64; Everett Rosenfeld, *The Controversial "Surveillance" Act Obama Just Signed*, CNBC, https://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html (last updated Dec. 22, 2015, 2:50 PM).

73. 6 U.S.C. § 1501(14).

74. *See id.* §§ 1501(6–7), 1504(c).

75. 6 U.S.C. § 1504(c); DHS & DOJ, *supra* note 24, at 3.

76. 6 U.S.C. § 1501(3).

77. *Id.* § 1502.

78. *Id.* § 1503(c).

also authorized to operate DMs within their respective systems and networks,[79] and to monitor their own systems and networks and the systems and networks of other NFEs or federal entities, provided they are authorized by those entities to do so.[80] The term "monitor" is given an expansive meaning under CISA, including "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system,"[81] for cybersecurity purposes.[82] CISA defines a cybersecurity purpose as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[83] Therefore, assuming that cybersecurity purposes would naturally include cyber-analysts' analyses of data collected through authorized monitoring activities, a textualist interpretation of these provisions suggests that the CISA-authorized monitoring includes, for cybersecurity purposes, the collection, possession, and analysis of ROD.[84]

3. Immunity from Suit for Acts of Sharing or Monitoring

Andrew Nolan reported to Congress that "[p]erhaps the most heavily debated legal issue respecting cyber-information sharing legislation is how to adequately minimize the host of liability issues that may arise for those in the private sector that may wish to disclose cyber-intelligence to outsiders."[85] Through its authorization for NFEs to share CTIs and DMs that may contain private information, CISA creates liability risk for program participants. Actions could be brought under the Electronic Communications Privacy Act of 1986 with relation to the monitoring of systems and networks and under federal or state privacy laws with relation to data being shared. Further, under the Sherman Antitrust Act, NFEs could incur criminal or civil liability for the sharing of CTIs and DMs as those actions could be construed as a "group boycott, or concerted refusals by traders to deal with other traders."[86]

To address this issue, CISA includes liability protection for participants sharing cyber threat intelligence under the statute. This immunity is an essential provision of the statute, as no reasonable NFE would participate in the program otherwise. A tailored approach to providing such liability protection may well have been impossible to craft, as drafters would have needed to apply forethought into all the legal theories under which NFEs could have incurred

79. *Id*. § 1503(b).
80. *Id.* § 1503(a).
81. *Id.* § 1501(13).
82. *Id.* § 1503(a)(1).
83. *Id.* § 1501(4).
84. *See supra* Subpart I.A.3 (providing a detailed definition of ROD). As neither Westlaw nor Lexis show any cases citing to any CISA provisions at this time, the interpretation of the CISA text has yet to be argued before the courts.
85. NOLAN, *supra* note 3, at 48.
86. 15 U.S.C. § 1 (2018); Klor's, Inc. v. Broadway-Hale Stores, Inc., 359 U.S. 207, 212 (1959).

liability for their acts under CISA.[87] Therefore, Congress chose to apply "broad immunity" from criminal and civil liability for NFEs' lawful acts under CISA.[88]

4. No Authorization for the Sharing of ROD

Conspicuously missing from the list of authorized acts under CISA-defined monitoring are the acts of giving or sharing of ROD—an NFE sending data already collected by itself through a monitoring process of its own network to a third-party.[89] Although the statute authorizes third-parties, presumably cybersecurity companies, which are NFEs in their own right, to harvest ROD through monitoring activities and to analyze that data for cybersecurity purposes,[90] it does not explicitly authorize NFEs or federal agencies to *send* their data to such third-parties for that same purpose.[91]

This confusing interpretation of the data sharing authorized under CISA is evidence of ambiguity in the meaning of the statute. In case of a dispute, the courts would likely first apply a textualist interpretation through the plain meaning rule.[92] Thus, in the absence of an explicit authorization for an NFE to send ROD previously collected on its own network to a third party, a textualist interpretation of CISA-defined *monitoring* requires that we infer that Congress never intended to authorize an NFE to send ROD that it collected on its own systems. There are good reasons for such an interpretation, as consumers' privacy rights could easily be trampled if every NFE was authorized to send any data collected on its own systems, even if that authorization was explicitly limited to cybersecurity purposes only. On the other hand, drawing a textualist distinction between authorizing a third-party to monitor an NFE's systems and thereby harvesting and transporting any data so captured, and an NFE monitoring its own systems and then sending that data to another NFE, that is, a cybersecurity firm—the activity not explicitly authorized—seems like a distinction without a difference. In both cases, the ROD is harvested in the same place and would likely end up in the possession of the same third-party. The only subtle difference rests in which party initiates and performs the initial data collection.

In the absence of a clear textual meaning of a statute, one of the parties in a controversy might ask the courts to apply alternative interpretations, including intentionalist and purposivist interpretations.[93] At the time Congress was considering CISA, the Congressional Research Service prepared a detailed

87. NOLAN, *supra* note 3, at 49.

88. 6 U.S.C. § 1505; NOLAN, *supra* note 3, at 50.

89. 6 U.S.C. § 1501(13).

90. *See supra* Subpart I.C.2 (detailing the data sharing schemes authorized under CISA).

91. *See supra* note 84 for a brief discussion regarding the lack of cases citing to CISA, hence this interpretation that would preclude any authorization for the sharing or sending of ROD has yet to be argued or disputed before the courts.

92. LINDA D. JELLUM, MASTERING STATUTORY INTERPRETATION 80–85 (Carolina Academic Press ed., 2d ed. 2013).

93. *Id.* at 197–229.

report providing perspective on an escalating cybersecurity risk landscape, on the existing legal framework supporting the sharing of cyber threat intelligence or lack thereof, and on the features of various proposed alternative legislative options considered.[94] While the report illustrates a thoughtful approach in determining the types of data to be shared, such as CTIs and DMs at the exclusion of ROD,[95] the report offers little to no insight regarding the various possible interpretations of the act of monitoring, rendering an intentionalist interpretation fruitless.

The courts may further seek meaning through an interpretation of the purpose of the statute as may be inferred from the broader context of its passage. Citing examples of recent prominent breaches, Congressional materials suggested that the "stated priorities of the President and congressional leadership [was] to enact laws that ensure that both the public and private sector are prepared to meet the cyber-challenges of the future."[96] Given such a broad mission and scope, one could be tempted to apply an equally broad interpretation of the definition of *monitoring*. However, the risks to privacy under such a wholesale data sharing authorization would be so great, even if limited to cybersecurity purposes only, that the courts would likely dismiss that interpretation. Therefore, as intentionalist and purposivist interpretations provide little to no additional guidance, we are left with the unsatisfying textualist interpretation defined above.

The resulting gap in explicit authorization for the sending of ROD creates a corresponding gap in the immunity afforded to NFEs under CISA.[97] In the absence of the immunity afforded by CISA, an NFE could have incurred liability under the Sherman Antitrust Act for acts of sharing CTIs containing IOCs identifying third-parties with whom the NFE perceived risk of communication.[98] The sharing of ROD, on the other hand, which is void of the negative judgment inherent to CTIs, poses minimal risks under the Sherman Antitrust Act, but risks of actions brought under federal and state privacy laws remain. This lack of immunity for the sending of ROD under CISA effectively precludes those

94. *See generally* NOLAN, *supra* note 3.

95. In its assessment of available options, the report suggests that

> The broadest approach is epitomized by bills like the Cybersecurity Information Sharing Act of 2014 (CISA), which would allow entities to share information about (1) cyber-vulnerabilities, (2) cyber-threats [together CTIs], *and* (3) broader efforts and strategies that have been used to prevent or mitigate cyberattacks, encompassing nearly any type of information within an entity's possession that merely pertains to cybersecurity [or DMs]. A more narrow approach would be that of proposals like the (CTSA), which allows public and private entities to share only limited types of cyber-threat information and does not contemplate entities sharing cybersecurity strategies [or DMs] with each other.

Id. at 44 (citations omitted).

96. *Id.* at 3.

97. *See infra* Subpart II.B (outlining the impact such ambiguity has on the private sector's willingness to share data for cybersecurity purposes).

98. *See supra* Subpart I.C.3.

activities except in the narrow circumstance of authorized third-party monitoring.

II. THE POST-CISA CYBERSECURITY CONTEXT AND THE ADVENT OF AI

The post-CISA facts do not bode well for Internet security. In the words of the Senate Select Committee on Intelligence in March 2017:

> The serious and growing number of cyber threats has been the subject of significant [Intelligence] Committee oversight and extensive testimony from senior [Committee] officials. The Committee has reviewed many troubling cybersecurity incidents and focused considerable attention on malicious actors' efforts in cyberspace to inflict harm in the short term, and to intensify their capabilities over the long term. . . . Foreign cyber actors have stolen sensitive U.S. national security information and valuable commercial information for intelligence purposes and economic gain. The Committee has noted with growing concern a trend in cyber activity: intrusions into sensitive government systems and critical infrastructure. The potential for a disruptive or destructive attack on our infrastructure continues to be one of the most significant cyber threats facing the United States.[99]

While the committee's assessment may sound dire, post-CISA cyber events suggest much work is left to be done to ensure the security of service providers and users alike.

A. AN ESCALATING CYBER THREAT LANDSCAPE

1. Cyber-Attacks Are Expanding in Size and Scope

The illicit acts of cyber-criminals and belligerent nation-state actors in cyberspace seem poised to continue. The authorizations afforded by CISA seem to have had a muted effect, if any, on the cyber-crimes committed. Although we cannot know how much damage would have otherwise been allowed absent the passage of CISA, "[t]he private sector continues to be plagued by cyber incidents ranging from systems hacking to poor practices that leave companies' information exposed. In the U.S. alone, the financial loss from cybercrimes exceeded $1.3 billion in 2016."[100] Focusing exclusively on technical cybersecurity, as opposed to content-based information security risks,[101] notable examples of cyber-attacks reported during the past two years include the Yahoo

99. S. REP. NO. 115-13, at 2 (2017).

100. Riley Walters, *Issue Brief: Private Sector Cyber Incidents in 2017*, HERITAGE FOUND., (Jan. 3, 2018), https://www.heritage.org/sites/default/files/2018-01/IB4803.pdf.

101. Leonhard Kreuzer, *Disentangling the Cyber Security Debate*, VÖLKERRECHTSBLOG (June 20, 2018), https://intr2dok.vifa-recht.de/receive/mir_mods_00003762 (differentiating between technical cybersecurity, a function necessary to protect the computing systems and networks of an organization, and content-based cyber-risks, which are best illustrated by fake news and influence campaigns in social media).

email breach,[102] expanded North Korean attacks,[103] the Equifax breach,[104] and the most devastating cyber-attack in history—NotPetya.[105]

Most organizations now transact using the Internet, almost universally collecting data about their customers in amounts proportional to their level of success. That collected data provides an increasingly attractive target for nefarious actors looking to profit from acts of data theft. This conundrum suggests that conducting a successful business will almost invariably lead to criminal intrusion attempts,[106] some through virtually any means possible.[107] Therefore, as long as organizations continue to expand their use of the Internet to deliver services to their users, every effort must be made to improve the security profile of their systems and networks. Given the post-CISA acceleration of cyber-crimes, achieving such improvements will likely require a step-function in the effectiveness of cyber-defenses.

---

102. In 2016, shortly after the enactment of CISA, we learned about the 2013 Yahoo email data breach that compromised every single Yahoo, Tumblr, Fantasy, and Flickr account—three billion in all. Selena Larson, *Every Single Yahoo Account Was Hacked—3 Billion in All*, CNN (Oct. 4, 2017, 6:36 AM), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html. Although Yahoo disclosed some information about the attack in 2016, the public did not learn of the full impact of that attack until months after Verizon had completed its acquisition of Yahoo. *Id*.

103. Following on its brazen attack against Sony Pictures Entertainment, see Sony Pictures, *supra* note 52, through its agents, the North Korean government continued a campaign of cyber-attacks against a variety of victims largely for financial gain. *See* Criminal Complaint, *supra* note 51, at 3 ("[There was allegedly a] wide-ranging, multi-year conspiracy to conduct computer intrusions and commit wire fraud by co-conspirators working on behalf of the government of the Democratic People's Republic of Korea"). These included the release of the WannaCry global ransomware and the cyber-heist of the bank of Bangladesh. *Id.* at 4–5. Despite what appears as a collaborative relationship between President Trump and the North Korean leader, in September 2018, "[t]he U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) . . . sanctioned one entity and one individual tied to the Government of North Korea's malign cyber activities." Press Release, U.S. Dep't of the Treasury, Treasury Targets North Korea for Multiple Cyber-Attacks (Sept. 6, 2018) https://home.treasury.gov/news/press-releases/sm473.

104. In 2017, one of the three nationwide credit bureaus that collect and report on consumers financial worthiness was the target of a cyber-attack that exposed the private financial data of up to 143 million people. "The attack on the company represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since 2015." Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

105. Allegedly developed and released by the Russian military in June 2017, this cyber-attack was the most devastating in history. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018, 5:00 AM), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Originally aimed at Ukraine's critical infrastructure, "[w]ithin hours of its first appearance, the [NotPetya] worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania." *Id.* "The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former Homeland Security adviser Tom Bossert, who at the time of the attack was President Trump's most senior cybersecurity-focused official." *Id.*

106. *See Not If, but When*, COUNCIL ST. GOV'TS (CSG Fiscal & Econom. Dev. Policy Program, Wash., D.C.), July/Aug. 2017, https://www.csg.org/pubs/capitolideas/enews/cs17_1.aspx.

107. *E.g.*, Elizabeth Weise & Chris Woodyard, *Home Depot: Card Breach Put 56M Cards at Risk*, USA TODAY, https://www.usatoday.com/story/tech/2014/09/18/home-depot-credit-card-breach-56-million/15843181/ (last updated Sept. 19, 2014) (detailing the extraordinary efforts and creativity hackers exerted in order to penetrate Home Depot's computer systems).

2. Ever-Evolving Cyber-Attack Designs

Continually looking to improve the effectiveness of cyber-attacks, cyber-criminals and nation-state actors evolve their techniques and intrusion technologies. For decades, the introduction of malicious code, through one means or another, has been a common and successful form of cyber-attack. Therefore, any robust cybersecurity infrastructure naturally included an anti-virus detection capability that would examine files on an organization's systems or networks to detect malicious code,[108] the most effective means of detecting cyber-attacks that required some form of code execution on the target organization's systems.[109] The year 2017 saw the advent of malware-less cyber-attacks, which are enabled through existing, authorized code execution pathways and no longer require the introduction of a file containing malicious code into the target organization's systems to be effective.[110] This new type of cyber-attack introduces another dimension of risk to organizations' systems and networks, as the anti-virus detection capabilities organizations have so heavily relied on may become obsolete.

B. LIABILITY CONCERNS INHIBIT INTELLIGENCE SHARING

Adding to the increasing frequency and strength of cyber-attacks, organizations appear to fail to leverage the intelligence sharing schemes available to them under CISA. Despite the fact that cyber "[t]hreat intelligence sharing is believed to improve the security posture of organizations and the nation's critical infrastructure,"[111] "potential liability . . . keep[s] some organizations from fully participating."[112] It is unclear whether these concerns are due to a lack of understanding of the legal immunity provided by CISA for the sharing of CTIs and DMs, or due to the ambiguity in the types of data for which CISA provides authorization. For example, if an NFE has logged a list of IOCs but has yet to draft complex CTI data structures for these IOCs, that NFE would likely be liable if one of its cyber-analysts chose to share that list with a peer NFE as these would not be properly formatted CTIs. Such ambiguities likely have some measure of chilling effect on any non-CTI and non-DM—in other words, ROD—sharing among NFEs since such sharing is technically not authorized under CISA. As a result, as long as the cybersecurity community's understanding of the immunity afforded to NFEs for their acts of sharing does not improve, the effectiveness of the intelligence sharing authorized by CISA will likely remain muted. Moreover, as the most likely interpretation of the CISA

108. *See supra* Subpart I.A.1.

109. *See supra* note 32.

110. Michael Viscuso, *What Is a Non-Malware (or Fileless) Attack?*, CMWARE CARBON BLACK (Feb. 10, 2017), https://www.carbonblack.com/2017/02/10/non-malware-fileless-attack/.

111. PONEMON INST., THIRD ANNUAL STUDY ON EXCHANGING CYBER THREAT INTELLIGENCE: THERE HAS TO BE A BETTER WAY 4 (2018).

112. *Id.* at 5.

text suggests no immunity is afforded to NFEs for the sharing of ROD,[113] it is even more likely that little to no ROD will be shared among NFEs except the ROD collected by third-party cybersecurity firms authorized to monitor other NFEs' networks.

As a result, NFEs have limited choices. Analogizing again to castle defenses, one option is for NFEs to collect their own ROD, with the limited visibility afforded from their own castle walls, and to analyze that ROD by further enriching it with the cyber threat intelligence provided through CTIs and DMs received from other castle owners or through fee-based cyber threat intelligence data feeds. NFEs choosing this option would not directly benefit from the ROD collected from the walls of neighboring castles; thus, their analyses would lack the perspective of footprints left in the snow at or around those neighboring castles. This option is equivalent to castle defenders being limited to line-of-sight visibility and to reports received from allies who have successfully identified nefarious actors (CTIs) and how to defend against them (DMs), a process fraught with shortcomings such as limited allies, likely time delays in the development and delivery of reports, and generally poor situational awareness.

Alternatively, NFEs could authorize third-party cybersecurity firms to monitor their respective information systems and networks with the expectation that those firms will have superior aggregate visibility. In that case, cybersecurity firms are akin to feudal lords providing protection to a network of castles, benefiting from the aggregate intelligence derived from the analysis of ROD collected across the network of castle defenses for which they are responsible. Cybersecurity firms, in turn, leverage the cyber threat intelligence developed through this aggregation of ROD as a competitive advantage to attract new clients.[114] Unfortunately, these strategies then preclude such firms from freely sharing the CTIs and DMs so derived, as these have become part of these firms' value proposition.

The net effect of such limited ROD sharing, therefore, is that NFEs are either limited to the perspective available from their own castle walls, or enjoy the expanded perspective and protection offered by a cybersecurity firm. The latter certainly allows the limited number of clients of a given cybersecurity firm to leverage the value of collected ROD, but that leverage of value is generally limited to the finite number of clients of that cybersecurity firm and no more.

C. THE ADVENT OF ARTIFICIAL INTELLIGENCE

The challenges associated with the acceleration of cyber-attacks, the evolution of cyber threats, and the chilled participation in cyber threat

113. *See supra* Subpart I.C.4 (explaining the reason to conclude CISA does not authorize the sharing of ROD among NFEs or between NFEs and the federal government).

114. *E.g.*, *FireEye Threat Intelligence: The Difference Between Informing Your Business and Informing an Appliance*, FIREEYE, https://www.fireeye.com/solutions/cyber-threat-intelligence.html (last visited Jan. 24, 2020).

intelligence sharing together present a daunting challenge to Internet security. The advent of AI and the leverage of such technologies by nefarious actors will likely accelerate and amplify these risks. Therefore, despite the news headlines being filled with references to AI and its positive implications to our daily lives, for the purpose of this Note it is important to understand the basic attributes of AI systems and their potential applications to the domain of cybersecurity.

1. From Chronically Emerging to Ubiquitous

In his recent book entitled *AI Super-Powers: China, Silicon Valley, and the New World Order*, Dr. Kai-Fu Lee details the history of AI research since his days as a doctoral candidate at Carnegie Mellon University in the 1980s, the struggles AI researchers had to overcome to produce useful technologies, and the implications of societies' broad adoption of AI for today and tomorrow.[115] Dr. Lee is the Chairman and CEO of Sinovation Ventures and President of Sinovation Venture's Artificial Intelligence Institute. Prior to founding Sinovation in 2009, Dr. Lee led Google China as its President and had previously held executive positions at Microsoft, SGI, and Apple.[116]

Research into artificial intelligence started as early as the 1950s, the dawn of the computer age.[117] By the 1980s, "the field of [AI] had forked into two camps: the 'rule-based' approach and the 'neural networks' approach."[118] The former attempted to "teach computers to think by encoding a series of logical rules," whereas the latter attempted to simulate the human brain itself, enabling computers to learn from exposure to "lots and lots of examples of a given phenomenon."[119] Unfortunately, for decades both of these approaches were plagued by resource constraints.[120]

"What ultimately resuscitated the field of neural networks . . . were changes to two of the key raw ingredients that neural networks feed on, along with one major technical breakthrough."[121] "Neural networks require large amounts of two things: computing power and data."[122] The latter provides the numerous examples the neural network needs to learn from, and the former provides the power to sift through those numerous examples.[123] Both data and computing power were historically in short supply, but today our smartphones provide millions of times more processing power than NASA used to put Neil Armstrong on the moon, and the Internet activity of billions of users has led to

115. *See generally* KAI-FU LEE, AI SUPER-POWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER (2018).

116. *About Dr. Lee*, AI SUPERPOWERS, https://aisuperpowers.com/about/about-dr-lee (last visited Jan. 24, 2020).

117. LEE, *supra* note 115, at 7.

118. *Id.*

119. *Id.* at 7–8.

120. *Id.* at 8–9.

121. *Id.* at 9.

122. *Id.*

123. *Id.*

an explosion of available data.[124] Moreover, the wide adoption of the Internet for daily use has dramatically increased the amount and variety of data available to data scientists as "[m]ore data has been created in the past two years than in the entire previous history of mankind."[125] In parallel, scientists achieved a significant breakthrough in neural network technology with vastly more efficient computer training capabilities.[126] These advances in infrastructure, data availability, and efficiency in computer training have set the stage for an explosion in the applications of AI across a range of industries including cybersecurity.

2. Neural Networks and Deep Learning

If a neural network is designed to learn like a human and to exhibit human-like behavior once taught, then it must be trained by exposing it, like a human, to vast amounts of data thus transforming it into a functional AI system.[127] When the learning is focused on a very specific domain, such as voice recognition, data scientists will apply deep learning training techniques to further improve the effectiveness of the AI system.[128]

Deep learning "use[s] massive amounts of data from a specific domain to make a decision that optimizes for a desired outcome. It does this by training itself to recognize deeply buried patterns and correlations connecting the many data points to the desired outcome."[129]

> Doing this requires massive amounts of relevant data, a strong algorithm, a narrow domain, and a concrete goal. If you're short any one of these, things fall apart. Too little data? The algorithm doesn't have enough examples to uncover meaningful correlations. Too broad a goal? The algorithm lacks clear benchmarks to shoot for in optimization.[130]

An obvious and desirable application of neural networks and deep learning is to the detection of movements and actions of nefarious actors within an organization's network and across multiple organizations' environments.

3. Application of AI to Cybersecurity

"AI-based technologies provide deeper security than what humans alone can provide . . . [and t]he deployment of AI-based security technologies simplifies the process of detecting and responding to application security threats

---

124. *Id.*

125. John W. Baker & Steve Henderson, *The Cyber Data Science Process*, 2 CYBER DEF. REV. 47, 47 (2017).

126. LEE, *supra* note 115, at 9.

127. *See* Bernard Marr, *What Is the Difference Between Artificial Intelligence and Machine Learning?*, FORBES (Dec. 6, 2016, 2:24 AM), https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/#7963062f2742.

128. Bernard Marr, *What Is the Difference Between Deep Learning, Machine Learning and AI?*, FORBES (Dec. 8, 2016, 2:14 AM), https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#3c9596fd26cf.

129. LEE, *supra* note 115, at 10.

130. *Id.*

and vulnerabilities."[131] But given the nature of deep learning, its application to cybersecurity requires that very large amounts of raw evidence of system and network activity be made available to neural networks. This data is necessary to train neural networks to understand normal behavior in an organization's network, a baseline from which the AI system could then differentiate anomalous events associated with network breaches.

In light of AI's promise of improved efficiency and effectiveness in the hunt for cyber threats, an explosion of AI-based cybersecurity solutions is being brought to market by cybersecurity vendors, large and small.[132] However, "AI-based technologies improve [cyber]security but will not reduce the need for staff. Working together, AI and IT security personnel can have a positive impact on organizations' cybersecurity posture,"[133] but AI is unlikely to solve the critical shortage of cybersecurity expertise.[134] As a result, while AI may present one element of the solution needed to stem the acceleration of post-CISA cyber-attacks, further investment in the number and skills of cyber-analysts will continue to be required.[135]

4. AI-Enabled Cyber Threats

"While AI may be the best hope for slowing the tide of cyber-attacks and breaches, it may also create more advanced attacker tactics in the short-term,"[136] hence AI presents itself as a double-edged sword to the cybersecurity community. "Sixty-two percent of surveyed [2017 Blackhat][137] attendees believe that there is a high possibility that AI could be used by hackers for offensive purposes" by the end of 2018.[138] "In fact, as cybercriminals and nation-states begin using AI to increase the rate of attacks, the need for smarter solutions that can help human security teams keep up will only become more apparent."[139]

131. PONEMON INST., THE VALUE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY 4 fig.2 (2018).

132. *E.g.*, Lily Hay Newman, *AI Can Help Cybersecurity—If It Can Fight Through the Hype*, WIRED (Apr. 29, 2018, 7:00 AM), https://www.wired.com/story/ai-machine-learning-cybersecurity/ (characterizing the availability of AI-based cybersecurity solutions at the RSA security conference, the largest global conference dedicated to commercial cybersecurity solutions).

133. *Id.*

134. *See infra* Subpart II.D (outlining the critical shortage in trained cyber-analysts affecting organizations' ability to protect themselves).

135. *See infra* Subpart II.D.

136. The Cylance Team, *Black Hat Attendees See AI as a Double-Edged Sword*, THREATVECTOR: SPOTLIGHT (Aug. 1, 2017), https://threatvector.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html.

137. "Black Hat is the most technical and relevant information security event series in the world. For more than 20 years, Black Hat Briefings have provided attendees with the very latest in information security research, development, and trends in a strictly vendor-neutral environment." *About Us*, BLACK HAT, https://www.blackhat.com/about.html (last visited Jan. 24, 2020).

138. The Cylance Team, *supra* note 136.

139. *Id.*

Unfortunately, nefarious actors in cyberspace are learning to weaponize AI to serve their illicit purposes.[140] "AI can make attacks very evasive, very targeted, and . . . bring an entire[ly] new scale and speed to attacks, with reasoning, and with autonomous approaches that can be built into attacks to work completely independently from the attackers."[141] Therefore, while AI can serve the purpose of improving efficiency and accuracy in detecting cyber-attacks, we already know that AI can make attacks significantly more effective and accurate, and potentially more devastating.

> [T]he 9/11 Commission report characterized the failures that led to that attack on our country as a "failure of imagination." . . . [T]he failure to detect and disrupt the Russian government's weaponization of online platforms against the United States and our allies [could be characterized as] . . . a similar failure to imagine.[142]

Our nation has the opportunity, now, to address the cyber-risks associated with AI, but time is of the essence.

D. CRITICAL SHORTAGE OF CYBERSECURITY EXPERTISE

As cyber-risks escalate, organizations are increasing their commitments to their respective cyber-defenses, causing the number of cybersecurity jobs to more than triple over the next five years.[143] In fact, "[a]ccording to one estimate, by 2021 an estimated 3.5 million cybersecurity jobs will be unfilled. And of the candidates who apply, fewer than one in four are even qualified."[144] A survey of Chief Information Security Officers indicates that "[a]utomation improves cybersecurity posture but does not reduce the need for in-house expertise. Sixty-two percent of respondents say automation, [including] artificial intelligence[,] . . . is not going to reduce the need for IT expertise but will enhance the productivity and effectiveness of skilled staff."[145]

III. CISA AMENDMENT PROPOSAL

Given the chronic shortage of skilled cybersecurity analysts, unless something dramatic changes in the degree of automation and efficacy of cybersecurity solutions, the risks to organizations' systems and networks are

---

140. *See* Dan Patterson, *How Weaponized AI Creates a New Breed of Cyber-Attacks*, TECHREPUBLIC (Aug. 16, 2018, 9:25 AM), https://www.techrepublic.com/article/how-weaponized-ai-creates-a-new-breed-of-cyber-attacks/.

141. *Id.*

142. *Foreign Influence Operations and Their Use of Social Media Platforms: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. (2018) (statement of Laura Rosenberger, Alliance for Securing Democracy, the German Marshall Fund of the United States).

143. Steve Morgan, *Cybersecurity Talent Crunch to Create 3.5 Million Unfileld Jobs Globally by 2021*, CYBERCRIME MAG. (Oct. 24, 2019), https://cybersecurityventures.com/jobs/ (last visited Jan. 24, 2020).

144. Erin Winick, *A Cyber-Skills Shortage Means Students Are Being Recruited to Fight Off Hackers*, MIT TECH. REV. (Oct. 18, 2018), https://www.technologyreview.com/s/612309/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers/?source=download-metered-content (citing Morgan, *supra* note 143).

145. PONEMON INST., SEPARATING THE TRUTHS FROM THE MYTHS IN CYBERSECURITY 5 (2018).

only likely to escalate from current levels. AI can play an important role in addressing these concerns, at least in part, but Congress must decide the quality and quantity of data that will be made available to cyber-analysts to enable their AI-powered cyber-defenses.

A cyber-attack is rarely, if ever, a singular frontal attack against an organization's cyber-defenses. Instead, would-be cyber-criminals apply malicious reconnaissance, enumeration, penetration, exfiltration, and sanitation techniques,[146] for which stealth is a critical success factor. Importantly, and in keeping with military tactics, if a cyber-analyst could improve her situational awareness by extending her visibility to her virtual neighbors' castle walls in addition to her own,[147] then that analyst's ability to observe would-be attackers' movements and tactics would dramatically improve her chances of detecting and inhibiting that would-be attacker's actions at her own castle defenses. It could be very tempting to suggest that a cyber-analyst could just wait for her neighbors to publish CTIs and DMs based on their own perspective, but it is sometimes through the accumulation of observations across environments that one can finally discern modus operandi and attack patterns of a would-be nefarious actor.

A. AUTHORIZING ROD SHARING AMONG NFES

While AI is not positioned to completely displace humans in cybersecurity roles, it has become a very effective tool for detecting anomalies in massive amounts of data based on established patterns of normalcy, the very essence of cyber-attack detection.[148] AI can improve the efficiency and effectiveness of cybersecurity solutions, but only if these solutions are afforded the necessary data from which to learn.[149] Hence, Congress should amend CISA, authorizing NFEs to share ROD[150] among themselves with the same civil and criminal immunity currently afforded by CISA for the sharing of CTIs and DMs. Doing so would be tantamount to shining bright lights on all the footsteps in the snow left at or near all the castle defense systems of those choosing to share ROD, thus allowing cyber-analysts to observe the movements of would-be cyber-criminals as they perform pre-attack surveillance, or other suspicious acts,[151] *before* such actors effectively breach their respective castle defenses.

146. ANATOMY OF A CYBER ATTACK: THE LIFECYCLE OF A SECURITY BREACH, ORACLE 4–5 (2017) (detailing the phases of a cyber-attack and the attackers' motivation behind each step).

147. *See* KISSEL, *supra* note 12, at 185 ("Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.").

148. *E.g.*, Newman, *supra* note 132 (illustrating how AI is well-adapted to the challenges of detecting antivirus defense and malware scanning).

149. *See supra* Subpart II.C.2 (explaining how and why AI deep learning solutions require massive amounts of topic-specific data in order to be effective).

150. *See supra* Subpart I.A.3 (analogizing ROD to footprints in the snow left by network and system users, whether nefarious or not).

151. *See* ORACLE, *supra* note 146, at 5.

1. The Benefits Outweigh the Risks

In the absence of such a bold data sharing strategy, cyber-analysts will largely be left to defending their walls, limited to their respective visibility albeit possibly enriched by cyber threat intelligence received from others.[152] The organizations they aim to protect would continue to be condemned to being attacked first before pursuing the attackers by following the "breadcrumbs" left behind, much as certain technologists advocated in their letter to Congress in dissent to the passage of CISA.[153] This more limited strategy, which CISA affords us today, has proven to be of limited effectiveness in stemming the tide of cyber-crime.[154]

On the other hand, while an explicit authorization for NFEs to share ROD among themselves would enhance their respective situational awareness and resulting abilities to defend themselves, this recommendation comes at the cost of reduced privacy for consumers. Although true, this proposal lives at the tension point between consumer privacy and the protection of the data consumers deposit in trust with online service providers who are charged with securing that data. To deny NFEs the access to technologies and supporting data necessary to thwart modern AI-powered cyber-attacks would render hollow any calls to those NFEs for securing users' privacy, as nefarious actors will continue to prevail in the game of one-upmanship we have observed since the use of the Internet has gone mainstream.[155]

2. ROD Is Already Defined in the CISA Data Sharing Specification

The utility of ROD to cyber-analysts is nothing new. The DHS adopted STIX/TAXII as the technical specification for the CTI/DM data sharing requirements of CISA.[156] The version of that specification in general release at the time of the enactment of CISA did not include the notion of ROD,[157] except as an extension of a CTI data structure.[158] As of July 2017, ROD is now defined as its own type of data on equal footing with CTIs and DMs in the STIX 2.0 specification.[159] While the authors of the STIX 2.0 specification might not have necessarily envisioned the level of ROD sharing recommended herein, the utility

---

152. *See supra* Subpart II.B (explaining the consequences of lack of ROD sharing).

153. Letter from Ben Adida et al., *supra* note 67, at 1.

154. *See supra* Subpart II.A (providing an overview of the escalating cyber-crime landscape).

155. *See supra* Subparts I.B.1, II.A (providing a pre- and post-CISA overview of the cyber-crime landscape).

156. DHS & DOJ, *supra* note 24, at 3.

157. *STIX Release Archive*, MITRE CORP., https://stixproject.github.io/releases/archive/ (last visited Jan. 24, 2020) (showing May 15, 2015 as the release date for STIX 1.2).

158. *STIX 1.2*, MITRE CORP., https://stixproject.github.io/releases/1.2/ (last visited Jan. 24, 2020) (detailing the object classes included in the STIX 1.2 specification including the Indicator class (CTIs) but lacking the Observed Data class (ROD)).

159. *STIX™ Version 2.0. Part 2: STIX Objects*, OASIS (July 19, 2017), http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html#_Toc496714322 (showing, in sections 2.5 and 2.8, the Indicator and Observed Data class definitions, respectively).

of ROD to cyber-analysts was sufficient to elevate it to its own data object class within the STIX 2.0 specification.

3. The Federal Government Should Be Excluded from Receiving ROD

Under CISA, only NFEs are authorized to monitor the systems and networks of other NFEs or federal entities who have granted authorization for that monitoring.[160] By implication, the federal government is not authorized to monitor NFEs' systems and networks, and therefore does not have access to NFEs' ROD. This design choice supports a sound privacy argument, and privacy advocates likely argued for that limitation in the wake of the Snowden Disclosures.[161] For like reasons, the federal government should be excluded from any ROD sharing schemes under this proposal, leaving it no worse off than with the current CISA statute, still able to receive and share CTIs and DMs but not ROD.

4. ROD Sharing Is in the Public Interest

Sharing more personal data than is already authorized under CISA has deep privacy implications, and finding the appropriate balance of privacy parameters for the implementation of this recommendation is not without its challenges. The tension between the desire to maximize the public good of Internet safety and the robust protection of privacy rights is hardly unique to the domain of cybersecurity. In fact, similar tension is evidenced in tech giants' adoption of AI in the broader technology sense.[162] As the *AngelList Weekly* has described:

> The competition among tech giants over AI isn't just an arms race—it's a battle of philosophies. On one side, companies like Google—despite taking PR hits over user privacy concerns—are focused on providing the most ubiquitous, accessible AI-powered services. Their bet: Ease of use and accessibility will outweigh consumer privacy concerns. Others, like Apple, take the opposite stance, betting a strong focus on privacy will continue to be a differentiating factor for consumers.[163]

A similar battle of philosophies could be at play in response to this Note's recommendation.

U.S. decision-makers have not yet confronted the necessity to make PII available to cyber-analysts to ensure public Internet safety. However, Drs. Clare Sullivan and Eric Burger, Georgetown University researchers in law and computer science, respectively, have analyzed the tension between public Internet safety and privacy rights with respect to the sharing of IP addresses (a very specific kind of cyber-relevant ROD) in the context of the European

160. *See supra* Subpart I.C.2.

161. *See* Macaskill & Dance, *supra* note 59.

162. *Apple's Quiet AI Acquisition*, ANGELLIST WKLY (ANGELLIST, San Francisco, California), Nov. 21, 2018, https://angel.co/newsletters/apple-s-quiet-ai-acquisition-112118?email_uid=853898960&utm_campaign=platform-newsletter-112118&utm_content=view-online&utm_medium=email&utm_source=newsletter-newsletter&utm_term=.

163. *Id.*

General Data Protection Regulation (GDPR)[164] and its predecessor, the 1995 Directive.[165] It can be instructive to study this example because it parallels the question at hand, i.e., should public Internet safety outweigh the need for absolute privacy with relation to a very valuable kind of cyber-relevant PII such as an IP address? In their view,

> [T]he sharing of IP addresses as cyber-threat intelligence can be justified in the public interest under Article 6(1)(e) of the GDPR to which the notification requirements of Articles 13 and 14 do not apply.[166] Sharing of threat intelligence is in the public interest and that interest overrides the individual rights of a data subject under Article 8(1)[167] of the Charter of Fundamental Rights of the European Union which underpins the GDPR and its equivalent in the 1995 Directive as long as the concepts of necessity and proportionality-of-purpose are adhered to in respect of the design of the specific measures proposed.[168]

According to this analysis, European courts would likely rule against individuals bringing privacy actions against private or public entities logging or sharing IP addresses for cybersecurity purposes, a necessary response whose purpose is proportional to the threat, despite the fact that IP addresses may be considered personal information in certain circumstances.[169] Applying this principle of security-over-privacy to a CISA context, authorizing NFEs to share ROD containing authorized PII, such as IP addresses,[170] should be considered in the public interest as public Internet safety and the security of online users' private data should take precedence over their individual rights to privacy.

B. LIMITING PII SHARING THROUGH DATA SEGMENTATION/AUTHORIZATION

Acknowledging the need to respect individual privacy rights while enabling an effective ROD sharing model, this proposed CISA amendment should also include provisions for granular PII definitions, segmentation, and sharing authorization. Unlike the more recently enacted CCPA,[171] CISA does not explicitly define PII other than to require those sharing CTIs or DMs to

---

164. *See generally* General Data Protection Regulation, *supra* note 33.

165. *See* Clare Sullivan & Eric Burger, *"In the Public Interest": The Privacy Implications of International Business-to-Business Sharing of Cyber-Threat Intelligence*, 33 COMPUTER L. & SEC. REV. 14, 14 (2017).

166. General Data Protection Regulation Article 13 defines certain requirements placed on system operators for notifying system users when their personal data is being captured from them directly, whereas Article 14 defines certain notification requirements in the event users' personal data is acquired but not from them directly.

167. A "data subject" is defined as an identified or identifiable natural person. General Data Protection Regulation, *supra* note 33.at art. 4, § 1.

168. Sullivan & Burger, *supra* note 165, at 29.

169. *Id.* at 22–24 (reviewing a case where a German court dismissed a private citizen's claim of privacy infringement, holding that a dynamic IP address is not personal information if the mapping of the address to a person requires cross-reference information only obtainable from a third-party such as an ISP and therefore not associated directly with their person).

170. *See infra* Subpart III.B (outlining a proposal for the segmentation of the types of PII that should be authorized to be shared as ROD).

171. CCPA § 1798.140(o)(1) (offering a non-exhaustive, yet reasonably complete, list of the types of data the California legislature considered PII).

redact information the entity "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual."[172] This lack of specific PII definition and resulting vagueness in definition of CTIs and DMs fueled strong dissenting opinions while CISA was being debated.[173]

As pertains to cybersecurity, not all PII is made equal. For example, while IP and email addresses are often prized for their value to cybersecurity analysis, intimate personal data such as health or financial data rarely are, if ever. The drafters of the STIX 2.0 specification thought this matter through in detail and have produced a specification of those types of ROD that are relevant to cybersecurity analysis as of the release of that specification.[174] The use of the expanded STIX 2.0 specification would be a natural evolution of the CISA data sharing model as STIX is already defined as the data sharing specification for data shared through the DHS under CISA.[175]

Contrary to the existing CISA broad-brush approach, the recommended amendment should segment PII into two categories: cyber-relevant PII such as are defined in the STIX 2.0 specification[176] and more sensitive PII such as health and financial information. This improved definition and segmentation of PII should be made applicable to all types of data being shared under CISA, including CTIs, DMs, and ROD. This approach would provide much clearer bright-line rules for the sharing of PII, thus improving NFE participation as a result of reduced litigation risk and, at the same time, reducing users' privacy concerns as they will be more assured that the sharing of their most sensitive data not necessary to cyber-analysis will be strictly forbidden.

This proposed amendment itself need not be explicit in the definitions and segmentation of PII. Instead, Congress should direct the DHS, as part of its CISA stewardship role, to develop and maintain the details regarding PII definitions and segmentation as a set of regulations under standard APA rule-making

172. Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1502(b)(1)(E)(i).

173. One comment letter sent on behalf of many civil society organizations, companies, and security experts argued that "the definitions for 'cyber threat,' and 'cyber threat indicator,' [were] concerning because they [were] unnecessarily broad." Letter from Access et al., to Barack Obama, Former President of the United States (July 27, 2015), https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition%20Ltr%20Urging%20Pres.%20to%20%20%20CISA.8b33e2d86dc14780b35c9cde44a41797.pdf (urging President Obama to strongly oppose the Cybersecurity Information Sharing Act of 2015).

174. *STIX™ Version 2.0. Part 4: Cyber Observable Objects*, OASIS (July 19, 2017), https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html ("STIX Cyber Observables document the facts concerning what happened on a network or host, but not necessarily the who or when, and never the why. For example, information about a file that existed, a process that was observed running, or that network traffic occurred between two IPs can all be captured as Cyber Observable data."). The classes of observable data included in STIX 2.0 are non-exhaustive. *Id.* "Objects and properties not included in STIX 2.0, but deemed necessary by the community, will be included in future releases." *Id.*

175. *See supra* Subpart III.A.2 (detailing the adoption of STIX/TAXII as the technical specification for sharing data with the DHS under CISA).

176. *See supra* Subpart III.A.2.

procedures.[177] The non-exhaustive nature of the STIX 2.0 ROD specification would readily accommodate such a malleable approach to managing the definitions of various subsets of PII.[178]

CONCLUSION

CISA has had a muted effect on the continued escalation of cyber-attacks. Since its passage into law in late 2015, AI has emerged as a powerful technology capable of performing certain tasks better than humans, including some aspects of cybersecurity analysis. The value of AI to the execution of mundane tasks has not escaped the attention of cyber-criminals who have been weaponizing AI to their own benefit. The drafters of CISA failed to anticipate the data sharing requirements of AI-powered cybersecurity solutions required to counter this emerging weaponization. NFEs stand to benefit from expanded CISA data sharing authorizations to include ROD, allowing their cyber-analysts to gain vastly improved situational awareness. The proposal herein provides for such an expanded data sharing scheme among NFEs only, to the exclusion of the federal government. In an effort to improve the overall privacy profile of CISA, these recommendations also include a more refined definition and segmentation of PII and limiting the sharing of PII under CISA to authorized, cyber-relevant PII only. With these improvements, NFEs will be better equipped to construct the AI-powered solutions we will need to face tomorrow's cyber threats.

177. *See The Administrative Procedure Act (APA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/open_gov/Administrative-Procedure-Act.html (last visited Jan. 24, 2020).

178. *See supra* note 174.

***